The Corinthian

Volume 6 Article 2

2004

What Effect Does Spyware Have on Consumer Trust, and Will its Use Ever Be Acceptable?

James Anthony Hatton
Georgia College

What Effect Does Spyware Have on Consumer Trust, and Will its Use Ever Be Acceptable?

James Anthony Hatton
Master Management Information Systems

Dr. Stephen L. Payne
Faculty Sponsor

Abstract

Trust literature has been thoroughly developed [Pavlou, 2001; Agranoff, 1998; Robinson, S.L. and Rousseau, D.M, 1994] in the field of Information Systems. However, recent innovations in broadband networks and the growing popularity of the Internet has brought rise to software called spyware – a program that employs a user's Internet connection in the background without the user's knowledge or explicit permission. This study attempts to analyze spyware and explore the nature of its effect on consumer trust. Additionally, the research examines what controls, if any may make the use of spyware acceptable to the consumer.

1. Introduction

As the Internet evolves and technology improves, businesses are faced with a unique opportunity: the ability to watch consumers from a distance and record their likes, dislikes, purchases, and even abandoned purchases from the comfort of company headquarters. The amount of potential data is endless. This is all done without the user's knowledge with software called spyware - computer programs used to transmit data from a computer, or that have the capability of transmitting data, via the Internet without the explicit permission of the user to initiate such transmission [Post, 2001].

The data which is collected by spyware programs is extremely valuable in terms of marketing and understanding customer behavior. However, many consumer watch dogs feel its collection severely invades personal privacy. In today's world of advancing technology, depersonalization, and a growing population, the need for personal privacy is a growing concern [Smith, J., Milberg, S., Burke, S. 1996]. Privacy defined as "the ability of the individual to personally control information about ones self" [Stone, Gardner, 1983] is widely regarded as "one of the most important issues of the information age" [Mason, 1986; Smith, 1994]. Spyware is just an extension of the overall loss of privacy faced by society today.

2. Background on Spyware

There are currently two main viewpoints regarding the use of spyware. The first viewpoint (held by the industry) states that by gathering information on consumers, they will be able to more accurately determine a user's interests and therefore, what offers, such as advertisements, with

which to target them. The motivation being that an advertisement more inline with a user's interest will be more effective. The interests of the user are based on which web sites they have visited, and, once there, what they purchased or searched for. The second viewpoint voices concern regarding the use of the data that is collected. The main concerns studies [Smith, 1996] have shown are illustrated in Figure 1.

Consumers and consumer advocates state that personal privacy is a human right. Their contention is that consumers should be informed up front when information about their behavior online has the potential to be collected and should affirmatively indicate their permission [New York New Media Association, 2003].

Privacy has been defined as the right to be left alone and free of unreasonable personal intrusion [Turban 2000]. What causes much debate however, is what constitutes 'unreasonable personal intrusion.' The overall issue is one of freedom of consumer information versus the right to privacy. The difficulty is determining what is "personal" and what constitutes "unreasonable intrusion" [Laczniak/Murphy, 1993].

3. Literature Review

The concept of spyware or even Internet surveillance in general has only recently been coined and is relatively new in terms of literature. However, upon closer inspection, the core issues relating to spyware have long ago been conceived and well documented. Thus, privacy and trust have become two of the most prominent topics for research and discussion in the field of Information Systems.

Privacy research dates back to the 1960s/70s (e.g. Westin, 1967 and HEW, 1973), but the increasing power of computers and networks brings new concerns. In the past, privacy was protected by the bounds of what was humanly possible, but now computers have pushed back these bounds while at the same time pushing back the boundaries of personal privacy. Public opinion polls show increasing levels of concern regarding personal privacy among Americans [Equifax 1998, 1999, 2000].

Increasing use of the Internet and 'always on' connections (such as DSL and cable modems) further highlights these concerns. The rapid advan in technology and companies' use of said technology has led to legal problems and negative media attention because of privacy issues [Smith, 1994]. There is a crisis of confidence concerning the safety of the Internet as well as confidence in the practices of certain online businesses. From the viewpoint of the consumer, personal privacy and security of transactions are major concerns [Carson, 2000].

4. Conceptual Development

This study examines the effect spyware has on the trust of its users. Specifically the questions this research study will attempt to answer are:

1) What effect does spyware have on consumer trust?
   It is likely that consumer trust will be affected once the user realizes that their actions are under surveillance. This research study intends to find out whether they still place the same trust in the company (responsible for the installation of the spyware) as they did prior to the discovery of spyware.

2) Is the concept of spyware unacceptable or just the way it is currently used?
   Could spyware be used in a way which is both useful to the company and agreeable with the consumer? The large majority of spyware comes packaged with 'freeware' – software which can be downloaded and installed at no dollar cost to the user. However, this is not to say that it is free. On the contrary, the user pays for the software, not with money but with their consumer information – a valuable commodity. This question explores whether users would be willing, under the right conditions, to sacrifice part of their privacy in exchange for the functionality provided by the free software.

H1: Spyware reduces consumer trust in the company responsible for its installation.

Spyware is often bundled with other software. This software consists of core functionality and functionality for information gathering or 'spying'. The core functionality appeals to users and entices them to install the software, but with this software, comes the spyware. The users trust towards the company that designed the functional part of the software is likely to be negatively affected by spyware's infringement on their personal privacy. However, given that the user chose this software company's product implies some level of trust in the company's goods, prior to the discovery of spyware being installed by their product.

The Internet has received a large amount of publicity, both good and bad, and in both cases not all of it was deserved. Whatever the reasons, it is now clear that the most important element of the consumer-marketer relationship is the notion of trust [Stewart, Pavlou and Ward, 2000]. Trust can be defined as the subjective assessment of one party that another party will perform a particular transaction according to his or her confident expectations, in an environment characterized by uncertainty

[Gambetta, 1988]. This definition embodies the relationship between tru and spyware. When a user installs a piece of software, they are placing a certain amount of trust in the company that it will not damage their machine and will work as expected. Interaction between the user and the company also occurs in an environment characterized by uncertainty: the Internet.

The marketing, function of an organization, specifically online marketing, needs to be sensitized to the issues of consumer trust and personal privacy. To be successful, a company should be active in obtaining consumer trust and confidence. Only then will they be effective in communicating with consumers [Carson, 2000].

Consumer trust is a valuable commodity which should be protect ed [Bell, 2002]. Trust is much harder to build then it is to lose [Ring and Van de Ven, 1992]. Years of a trusting relationship can be sabotaged in one day through the invasion of a consumer's privacy; the negative effects of which may last a lifetime. Research concerning breaches of trust has shown trust will rapidly degenerate if the user perceives the trust violation is the trustee's 'normal' rather then aberrant behavior. If a consumer discovers they have spyware on their machine that was installed by software that they have been using for a substantial period of time this would not constitute aberrant behavior since the spyware was running since the date the original software was installed. However, if the software company sought to correct the matter, then the consumer may discount the inciden as abnormal behavior and the consumers trust would be less severely eroded. This was the case with Mattel who provided an uninstall program that removes software features designed to transmit and receive information to Mattel headquarters.

When a consumer chooses to install a software product, this implies a level of trust. This trust can be categorized as a "psychological contract" defined as an individual's beliefs regarding the terms and conditions of a reciprocal exchange agreement [Bell, 2002]. The software company has an obligation to provide software containing the same functionality as was advertised. Major deviations from this functionality (such as spyware) are deceptive. The discovery of spyware would most likely constitute a psychological violation. Negatively affecting a consumer's trust can result in emotional responses such as anger, resentment, and cynicism towards the trustee [Robinson and Rosseau, 1994]. These feelings would be directed at the software company responsible for the installation of the spyware as it is in this company that the consumer held some level of trust in the company's goods given that they chose their product.

Previously, trust was defined as the subjective assessment of one party that another party will perform a particular transaction according to his or her confident expectations [Gambetta, 1988]. When a user installs a

piece of software, they are placing a certain amount of trust in the company that the software will work as expected. What is not expected is for the software to 'spy' on them and once the users discover this it is the hypothesis of this study that their trust will be negatively affected.

H2: If implemented with mechanisms to control its use consumers would find the use of spyware acceptable.

It is likely that users would be willing to exchange their consumer information in exchange for software functionality. The industries' view of spyware contains some valid points, and based on the fact that you are going to see advertisements and receive solicitations regardless, it is likely that consumers would prefer to view those which matched their preferences. Before this is possible, however, user concerns would have to be accounted for (see Figure 1) and trust built that some level of personal privacy would be respected. The studies hypotheses are presented diagrammatically in the research model featured in Figure 9.

5. Methodology

5.1 Sample

A quantitative web-based survey was used to conduct the research. Administering an online survey has the disadvantage of limiting the sample to only those with access to the Internet. However, this did not have an adverse effect in this case since a requirement of this study was that its participants have access to the Internet; spyware cannot function without an active Internet connection.

Incidence was not a problem in this study as a large number of people have a connection to the Internet in the population area sample (United States and Europe). The survey was distributed to 67 Internet users. A convenience sample was used, and therefore, was unfortunately not random. The survey resulted in 26 usable responses, for a response rate of approximately 38%.

5.2 Measure Development and Validation

The existence of spyware remains a secret to most. Since it is impossible to measure the affect spyware has on a user without them knowing about it, questions were administered to determine if the user had installed packages known to contain spyware, and to find out if the user is aware of any spyware on their machine. A list of the most popular software packages containing spyware were shown to the user who was asked to select those which they use (see Figure 2 for details). Separate measures were then implemented to measure the constructs trust and acceptability.

Trust

The principle constructs were developed based on existing measures developed in previous literature where possible. Measures for trust were synthesized from Jarvenpaa, Tractinsky, Vitale (2000) in addition to those adapted from Smith, Burke, Milberg (1996) based on their work measuring individuals' concerns about organizational practices.

The measure was applied twice to the survey participants. Once the user had indicated the software he or she used, the trust in these software companies was measured. The user was then asked whether they were aware of any spyware on their computer. If he or she answered 'No', then the nature of spyware was then explained to them and a list of software packages containing spyware was displayed. Only those software packages which the user said he or she used was displayed. The measure was then applied again to see if the participant's new knowledge (that software they use is spying on them) affects the trust he or she holds in the companies who bundle the spyware with their product. Those participants who were aware of spyware on their computer were automatically redirected to the next section as the effect their knowledge of spyware had on their trust was captured by the initial measurement.

Acceptability

Existing measures for the acceptability of spyware were not available. Therefore, great care was taken to design a new measure designed to find out if users would find the idea of spyware more acceptable if certain controls were in place to control its use. A preliminary version of the instrument was generated, which was reviewed by faculty and graduate students for clarity and comprehensiveness.

The final measures for both constructs used in this research and their internal consistency results (Cronbach's alpha) are shown in Figure 3. As expected for a new measure, the reliability of the measure of ACCEPTABILITY (0.76) was lower than the measure used for TRUST (0.86). However, both measures were still above the .7 suggested by Nunnally (1978) for basic research. Factor analysis was conducted using varimax rotation. Items were removed which appeared to be measuring different aspects of the constructs. The factor analysis was repeated and all items tapping the same construct had high correlations, where as items tapping different constructs had significantly lower correlations. Each measure's remaining items loaded on their hypothesized factors and estimates were positive and significant (see Figures 4 and 5 for details). Therefore, convergent and discriminant validity for both TRUST and ACCEPTABILITY is supported.

6. Results

The items used to measure the construct trust were averaged to create a new variable. This was repeated for the results of the second application of the measure, resulting in two new variables TRUST and TRUST2. A paired-samples t test (see Figure 6 for details) was used to test the hypothesis that spyware reduces consumer trust in the company responsible for its installation.

The results of the paired-samples t test allow the null hypothesis that a company's use of spyware had no effect on consumer trust to be rejected. The null hypothesis can be rejected because 0 is not within the range of the 95% confidence interval and the significance level is below 0.05.

The measure of trust used a five-point likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The mean for the variable TRUST is 3.96 very close to 4 which is 'Agree'. The mean for TRUST2 is 2.81. This shows a significant reduction in trust of 1.15. Therefore, the alternate hypothesis that a user's trust is negatively affected by a company's use of spyware can be accepted.

A paired-samples t test was also used to test the second hypothesis that consumers would find spyware more acceptable if it was implemented with mechanisms to control its use (see Figure 7 for details). The variable R_NEVER is the question, "I would never use spyware" reverse scored since if the user disagrees, this indicates they would consider using spyware. Therefore, the question becomes, "I would use spyware." All items measuring acceptability were administered using the same five-point likert scale mentioned previously for TRUST. Once the results were reversed scored, the mean answer was 2.70.

The variable CONTROL represents the mean of the items used to measure how acceptable users find spyware if it was monitored by control mechanisms. The control mechanisms are (i) regulating its use with legal restrictions, (ii) anonymous data collection and (iii) the option to turn the spyware off. The variable CONTROL represents how acceptable the average user would find spyware if it was regulated by legal restrictions, all data collected was anonymous, and they had the option to turn it off.

The null hypotheses that spyware would never be acceptable even with mechanisms to control its use can be rejected as the significance of the paired-samples t-test is 0.03, below the required 0.05. The paired-samples statistics featured in Figure 5 show that mean values of R_NEVER and CONTROL are 2.73 and 3.58 respectively. The acceptability of spyware increases by 0.85 (3.58-2.73). Therefore, the alternate hypothesis that with controls mechanisms in place users find the use of spyware more acceptable, can be accepted.

6.1 Limitations of the Study

The primary limitation of this study is the type and size of the sample. A convenience sample was used due to financial and time-based constraints. Therefore, the sample contains unknown amounts of both systematic and variable error. In addition to the type of sample, the size of the sample is also relatively small containing only 26 useable responses. The study was non-experimental, and therefore, causation is not confirmed as the absence of other causal factors cannot be guaranteed. The data may have been affected by self-presentation biases, caused by members of the sample claiming knowledge of the existence of spyware, when in reality they were not aware. However, one might expect the nature of such presentation to be lower for this form of data collection when compared to other more personal, face-to-face settings.

7. Implications and Conclusion

The aim of this study was to measure the effect, if any, that spyware had on consumer trust towards the software company responsible for its installation. It is assumed that the user holds a certain amount of trust in the software company before the discovery of spyware. This is reasonable because the use of a product implies some level of trust in the company's goods. The second objective of this study was to discover if the use of spyware would be more acceptable to consumers if control mechanisms were in place to regulate its use.

The contributions of this research are two-fold. First, the research shows that if a software company includes spyware in its products, the trust the consumer holds for the company will be negatively affected. The United States does not have data protection laws and therefore, there is no legal recourse if a company promises privacy but does not honor its promises. Past researchers state that because companies know there is no legal enforcement, there is little incentive to amend company practices [Coyle, 1999]. Consumers have legitimate concerns concerning how their privacy is affected by organizational practices [Smith et al, 1996]. Consumer trust is a valuable commodity and companies would be wise to not risk negatively affecting it, no matter what legal restrictions are in place. Companies such as RealNetworks, a well known Internet multimedia firm, learned first hand the negative effects the use of spyware can cause. The software company inserted a new feature into RealJukebox that helps users more easily catalogue their own CD libraries. To do this, however, the program uploaded a unique identifier from the user's system to RealNetworks' servers, which identified the user and was used to track their actions. RealNetworks did not inform its users that the uploading was taking place. Early in 2000, RealNetworks became the "poster" child for its lack of privacy practices and found themselves facing a public relations disaster Carson, 2000].

The second contribution of this research is that consumers find spyware more acceptable if implemented with certain control mechanisms to regulate its use. The control mechanisms used in this research were (i) regulating spyware's use with legal restrictions, (ii) anonymous data collection, and (iii) the option to turn the spyware off. The results showed that with these control mechanisms in place, consumers found the use of spyware more acceptable.

If companies implement spyware, they can gather information on consumers that will enable them to determine a user's interests with greater accuracy and provide the capability of targeted advertising. The motivation being that an advertisement more inline with a consumer's interest is more effective. Before companies can implement spyware, they must enforce mechanisms to control its use. Ensuring all data collected is anonymous and giving the consumer the option to turn off the spyware are technical issues relatively easy to enforce. The establishment of legal restrictions is probably beyond the power of most companies. However, there are a number of private associations that have established themselves to help build consumer confidence in business practices. These associations such as TRUSTe, BBBOnline and Privacy Seal ask members to ascribe to certain standards in order to be assured that information practices are carried out with integrity. Other associations are advocacy groups to persuade business and government to make informed decisions related to privacy issues (see Figure 8 for details). The standards required by these associations may help alleviate consumers concerns until effective legal restrictions are in place.

In sum, the research shows that if a software company includes spyware in their products without appropriate control mechanisms, the trust the consumer holds for the company will be negatively affected. The results support the research model presented in Figure 9. In 2000 Carson suggested that privacy on the Internet be structured in the same way privacy is structured in accounting practices. Implicit guidelines are needed to capture widespread consumer trust. While international agreements regarding global legal restrictions are being agreed upon, firms should be taking the initiative to innovate toward a business evaluation of ethical values and ascribe to associations designed to help build consumer confidence in business practices.

7.1 Suggestions for Future Research

There are several ways in which future research could strengthen the results of this study. The results found by this research may be constrained by the limited sample size. The sample also contained both systematic and variable error so that future research using a probability design may be fruitful. Additionally, it was beyond the scope of this research to

measure the effect of a large number of control mechanisms on consumer acceptability. It is possible that there may be other control mechanisms which affect the acceptability of spyware to a much larger extent then the ones chosen here.

Works Cited

Agranoff, M.H., "Controlling the Threat to Personal Privacy," Journal of Information Systems Management, June 1998.

Ba, S., Pavlou, Paul. "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior." MIS Quarterly, September 2002.

Barnett. "Ethical ideology and the ethical judgments of marketing professionals." Journal of Business Ethics, June 2000.

Bell, G., Oppenheimer, R., Bastien, A. "Trust deterioration in an international buyer-seller relationship." Journal of Business Ethics, Mar 2002.

Bush. "Ethics and marketing on the Internet: Practitioners' perceptions of societal,industry and company concerns." Journal of Business Ethics, July 2001.

Carson. "Online Consumer Privacy The Effect of Technology on Ethics and Consumer Privacy in Internet Marketing." Ethical Issues of Marketing, July 2000.

Coyle, Karen. "P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences (P3P)." Retrieved June 30, 1999, from the World Wide Web: http://www.kcoyle.net/p3p.html

Dawe, S., Evans, W., Denney, M. "Top of the E-Class: Ranking and Best Practices of Over 170 Web Sites." Retrieved June 2000, from the World Wide Web: http://www.csca.ryerson.ca/publications/2000-04.html

Dunfee (1999). "Social contracts and marketing ethics." Journal of Marketing, July 1999.

Electronic Task Force, "Strategies, Privacy the Protection of Personal Information, Codes of Practice." Retrieved July 9, 2000, from the World Wide Web: http://e-com.ic.gc.ca/english/privacy/632d23.html

Equifax, Inc. "The Equifax Report on Consumers in the Information Age." 2000.

Gambetta, D. "Trust: Making and Breaking Cooperative Relations." Basil Blackwell, 1988.

Green, H. "Our Four-Point Plan." BusinessWeek. Retrieved March 2000, from the World Wide Web:http://businessweek.com/2000/00_12/b3673006.htm

HEW (U.S. Department of Heath, Education and Welfare). "Records, Computer and the rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Government Printing Office, 1973.

Jarvenpaa, S. L., N. Tractinsky and M. Vitale. "Consumer Trust in an Internet Store" Information Technology and Management, 2000.

Laczniak, Gene, and Murphy, Patrick (1993). "Ethical Marketing Decisions (the higher road)," Allyn & Bacon, Boston, 1993.

Mack. "Electronic marketing: What you can expect." The Futurist, Mar/Apr 2000.

Malmos, D. "Beware Spyware lurks on the web." Herald Business Journal, 2003.

Manning. "Playing the global name game." Target Marketing, Apr 2000.

Marshall. "Has technology introduced new ethical problems?" Journal of Business Ethics, Apr 2001.

Martin, D., Smith, R., Brittain, M., Fetch, I., Wu, H. "The Privacy Practices of Web Browser Extensions." Communications of the ACM, Feb 2001.

Mason, R. O. "Four Ethical Issues of the Information Age." MIS Quarterly, 1986.

Mitchell, S. "The New Age of Direct Marketing." Journal of Database Marketing, Apr 2003.

Nelson. "Business group takes on privacy." Information Week, Apr 10, 2000.

New York New Media Association (NYNMA). "The Privacy White Paper," 2003.

Pate, J., Malone, C. 'Psychological Contract Violation: The durability and transferability of employee perceptions: the case of TimTec." Journal of European Industrial Training, 2000.

Pavlou, P. "Integrating Trust in Electronic Commerce with the Technological Acceptance Model: Model Development and Validation." Seventh Americas Conference on Information Systems, 2001.

Post, A. "The dangers of spyware." Symantec Security Response, 2001.

Robinson, S.L. and Rousseau, D.M. (1994). "Violating the psychological contract: not the exception but the norm." Journal of Organizational Behavior, Vol. 14 No. 3.

Sibley. "Survey ties high-tech to unethical practices." Computing Canada, May 1998.

Singhapakdi. "Ethics gap: Comparing marketers with consumers on important determinants of ethical decision-making." Journal of Business Ethics.

Singhapakdi. "International marketing ethics." Journal of Business Ethics.

Smith, J. "Managing Privacy: Information Technology and Organizational America." University of North Carolina Press, 1994.

Smith, J., Milberg, S., Burke, S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." MIS Quarterly, June 1996.

Stone, E. F., Gardner, D. G. "Privacy In America: Is Your Life in the Public Eye?" MIS Quartley, 1983.

Thong. "Testing an ethical decision-making theory: The case of softlifting." Journal of Management Information Systems, Apr 2000.

Turban, Ephraim, Lee, Jae, King, David, Chung, H. Michael. "Electronic Commerce: A Managerial Perspective." Prentice Hall, Apr 2000.

Westin, A. F. "Privacy and Freedom." Antheneum Publishers, 1967.

Williamson. "Wanted: Info on you and your interests, MatchLogic to build giant data warehouse for targeted ads." Advertising Age, May 1997.

W3C. "Platform for Privacy Preferences (P3P Public Overview)." Retrieved June 30, 1999, from the World Wide Web: http://www.w3.org/P3P/

Figure 1

Concern	Description of Concern
Collection	Concern that extensive amounts of personally identifiable data are being collected and stored in databases.
Unauthorized Secondary Use (Internal and External)	Concern that information which is collected from individuals for one purpose, but is used for another.
Improper Access	Concern that data about individuals are readi ly available to people not properly authorized to view or work with this data.
Errors	Concern that the data is not properly checked for accuracy.
Reduced Judgment	Concern regarding increased automation of decision making processes.
Combining Data	Concern that personal data in disparate databases may be combined into larger databases thus creating a 'mosaic effect'.

Figure 2

Company Name	Software Name
Real Networks	RealDownload or RealJukeBox
Intuit	Quicken
Netscape and AOL	AOL Smart Download
NetZip	NetZip's Download Demon
Limewire	Limewire Peer to Peer File Sharing
Audio Galaxy	Audio Galaxy Music Sharing
Kazaa and Brilliant Digital	Kazaa Peer to Peer File Sharing
Bonzi	Bonzi Buddy Program
eXact Advertising	Bargain Buddy
Forbes	Forbes Business Alerts
Gator	Gator eWallet
GoHip	GoHip Movie Player
Target Interactive	Gratisware IE Plugin
Market Score	Market Score Internet Acelerator
Mindset Interactive	NetPay
newtonknows.com	Newton Knows Dog
Gigatech Software	SuperBar IE Plugin
Divago	SurFairy
surfmonkey.com	Surf Monkey
Bearshare	Bearshare Peer to Peer File Sharing
Imesh and Olenich Design Studio	Imesh Peer to Peer File Sharing
Grokster	Grokster Peer to Peer File Sharing
Xolox B.V	Xolox Peer to Peer File Sharing
Blubster Networks	Blubster or Piolet
OneMX Networks	OneMX

Figure 3

For the construct TRUST, participants were instructed to answer the questions based on the software companies whose software they ecked as using.

Item	Cronbach's alpha
TRUST	
The company or companies is/are trustworthy	
This company keeps its promises and commitments	
I trust this company to keep my best interests in mind	0.86
The company is known to be dependable	
The company has a poor reputation (reverse scored)	
ACCEPTABILITY	
I would never use software which contained spyware (reverse scored)	
I would use software which contained spyware if legal restrictions were in place to regulate its use	
I would use software which contained spyware if the data collected was anonymous, and pertained only to my demographic data, such as age, gender, and edu cation	0.76
I would use software which contained spyware if I have the option to turn it off	

Figure 4

Component Transformation Matrix

Component	1	2
1	.876	.482
2	-.482	.876

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Communalities

	Initial	Extraction
dependable	1.000	.730
companies_are_ trustworthy	1.000	.450
keeps_promises	1.000	.691
best_interests	1.000	.635
REPUTATI	1.000	.788

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.295	65.892	65.892	3.295	65.892	65.892
2	.795	15.897	81.790			
3	.539	10.779	92.569			
4	.200	4.002	96.570			
5	.171	3.430	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
dependable	.855
companies_are_ trustworthy	.671
keeps_promises	.831
best_interests	.797
REPUTATI	.888

Extraction Method: Principal Component Analysis.
a. 1 components extracted.

Figure 5

Communalities

	Initial	Extraction
if_legal_restrictions _were_in_place	1.000	.521
if_the_data_collecte d_was_anonymous	1.000	.825
option_to_turn_it_off	1.000	.695

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.042	68.065	68.065	2.042	68.065	68.065
2	.680	22.659	90.724			
3	.278	9.276	100.000			

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
if_legal_restrictions _were_in_place	.722
if_the_data_collecte d_was_anonymous	.908
option_to_turn_it_off	.834

Extraction Method: Principal Component Analysis.

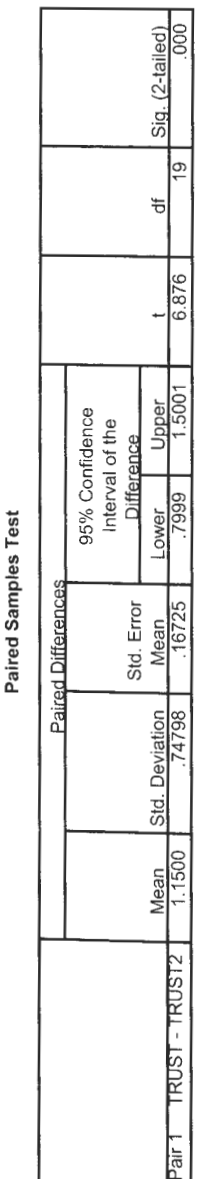
a. 1 components extracted.

Rotated Component Matrix[a]

a. Only one component was extracted. The solution cannot be rotated.

Figure 6

The paired-samples t test to test the hypothesis that spyware reduces consumer trust in the company responsible for its installation



Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	TRUST - TRUST2	1.1500	.74798	.16725	.7999	1.5001	6.876	19	.000

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	TRUST	3.9600	20	.54134	.12105
	TRUST2	2.8100	20	.70629	.15793

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	TRUST & TRUST2	20	.304	.193

Figure 7

The paired-samples t test to test the hypothesis that consumers would find the use of spyware acceptable if it was implemented with mechanisms to control its use

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	R_NEVER	2.7308	26	1.18516	.23243
	CONTROL	3.5897	26	.77349	.15169

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	R_NEVER & CONTROL	26	.122	.553

Figure 7 (cont.)

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	R_NEVER - CONTROL	-.8590	1.33391	.26160	-1.3978	-.3202	-3.284	25	.003

Figure 8

Associations whose mission it is to persuade business and government to make informed decisions related to consumer privacy issues

- The Electronic Privacy Information Centre
- The Electronic Frontier of Canada
- The Centre for Democracy and Technology
- The Internet Advertising Bureau
- Privacy.Net
- The Online Privacy Alliance
- Global Internet Liberty Campaign
- Beyond Concern
- Kidz Privacy
- PrivacyOnline.org
- Interactive Marketing Research Organization
- The Privacy Leadership Initiative
- The Privacy Rights Clearinghouse

Figure 9

Research Model